

> Leveraging an Identity Management Foundation to Sustain Compliance

June 10, 2008

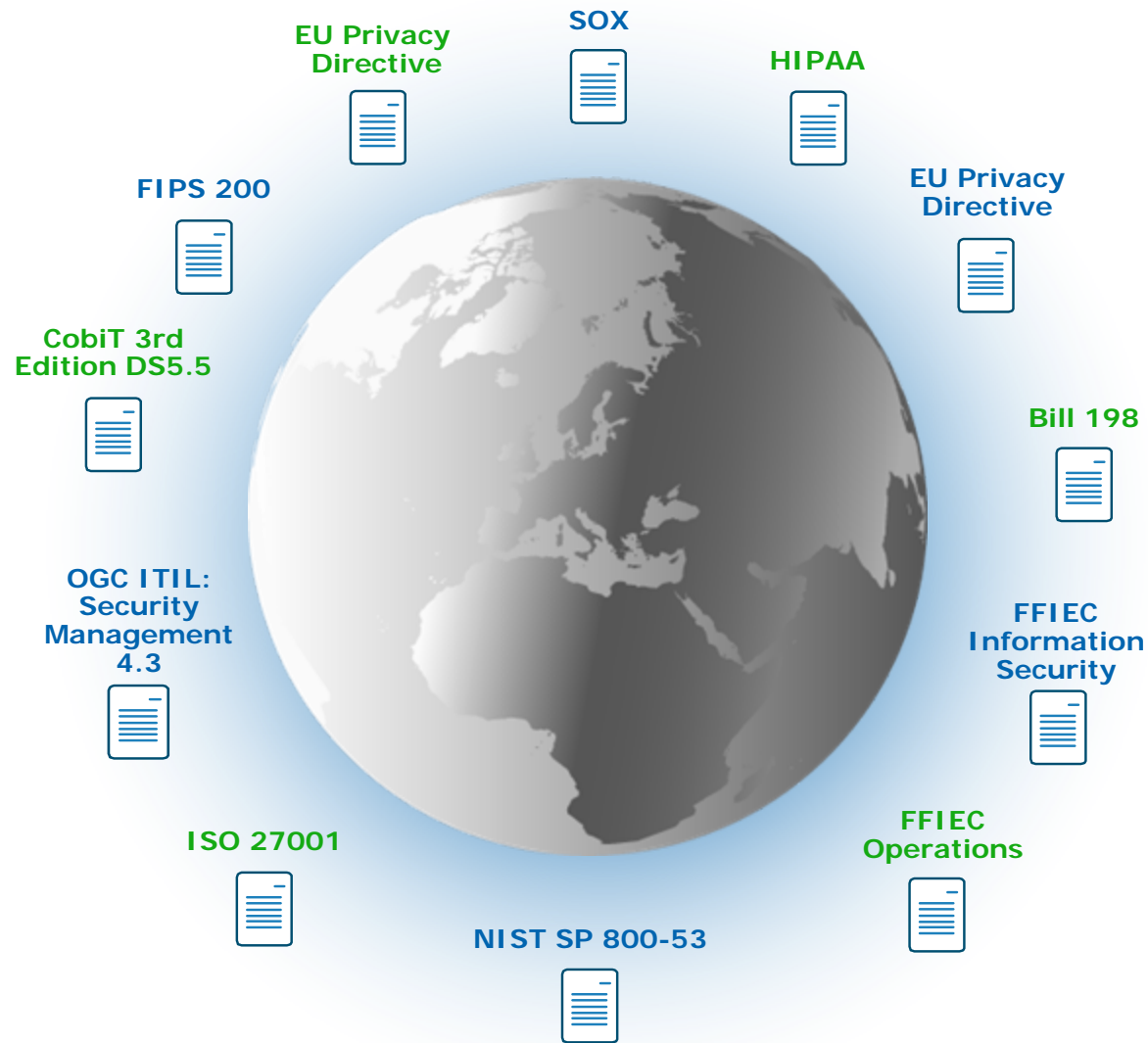
Agenda

- > The challenge of managing multiple users and entitlements
- > Identity Lifecycle Management defined
- > Three components
 - Identity Management
 - Security Compliance Management
 - Role Management and Role Engineering
- > CA customer perspectives



The Regulatory Environment

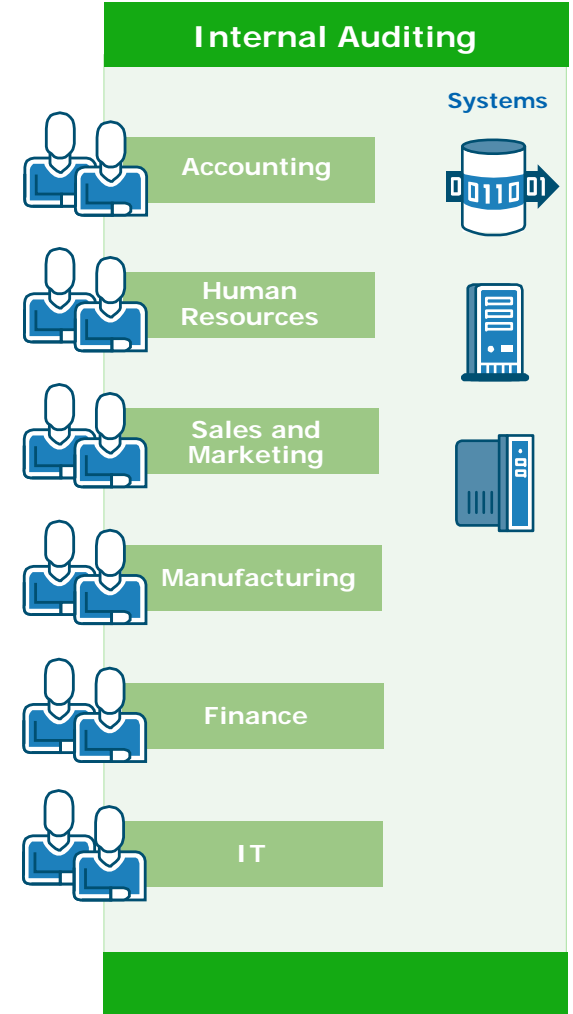
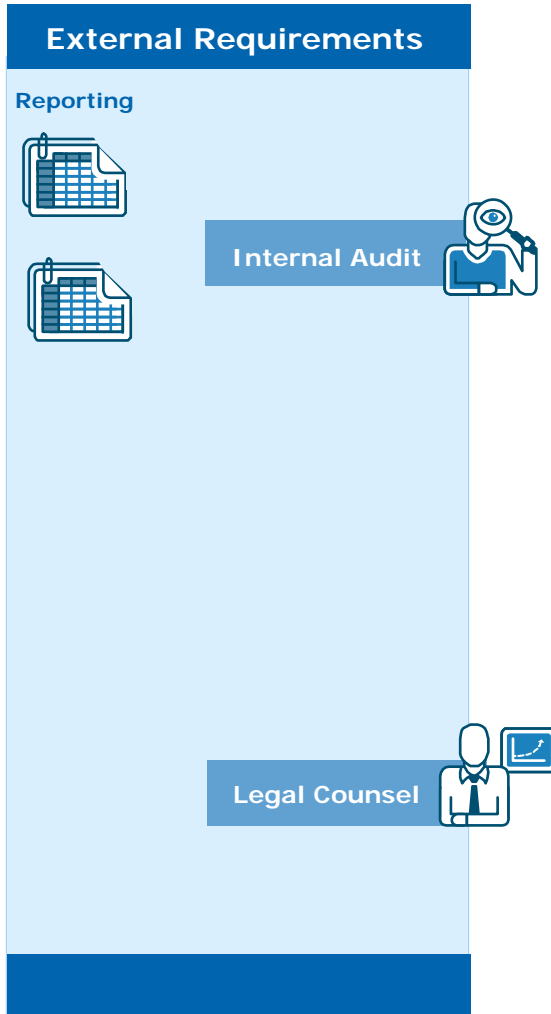
Global and Growing





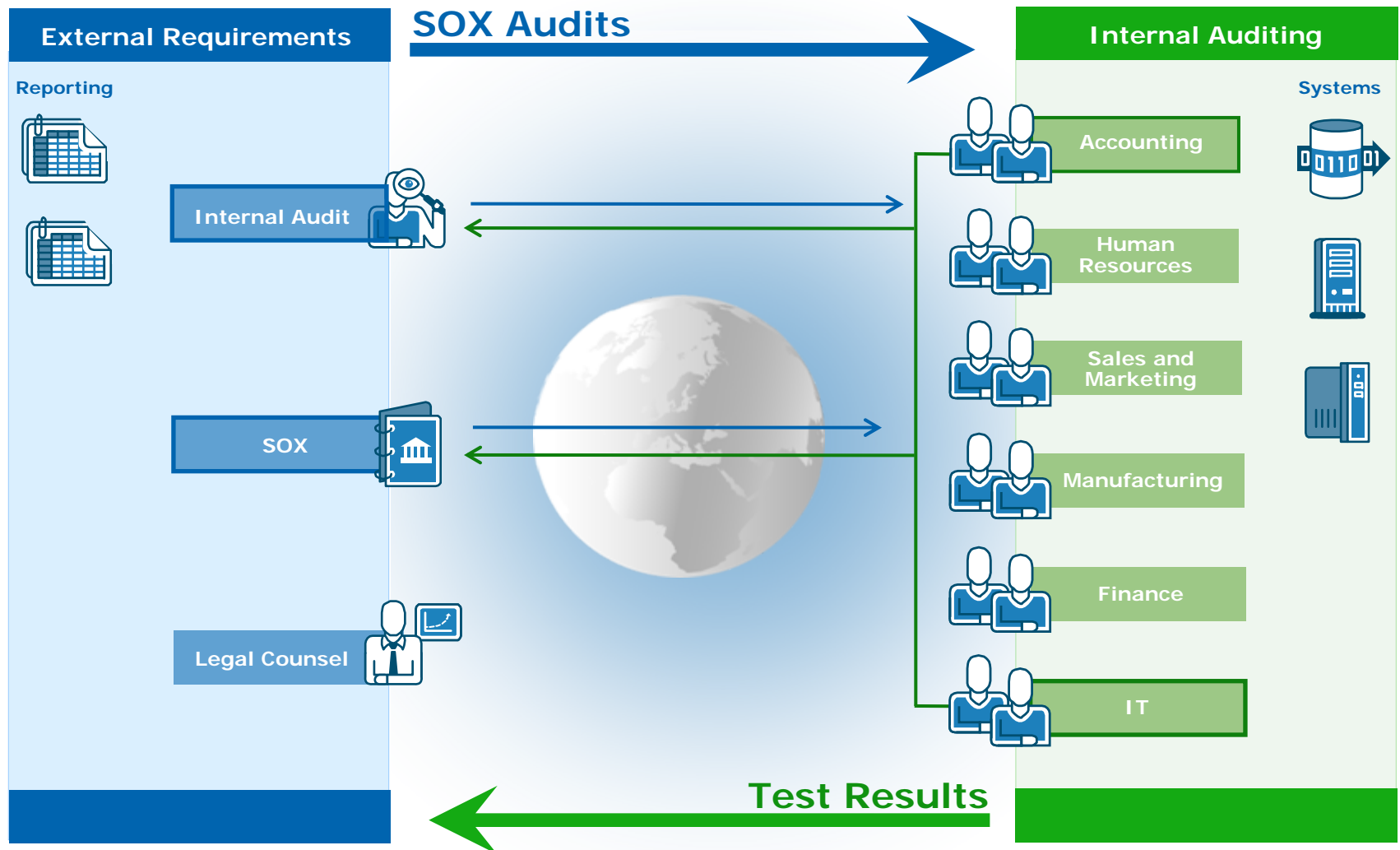
Compliance

The Early Days



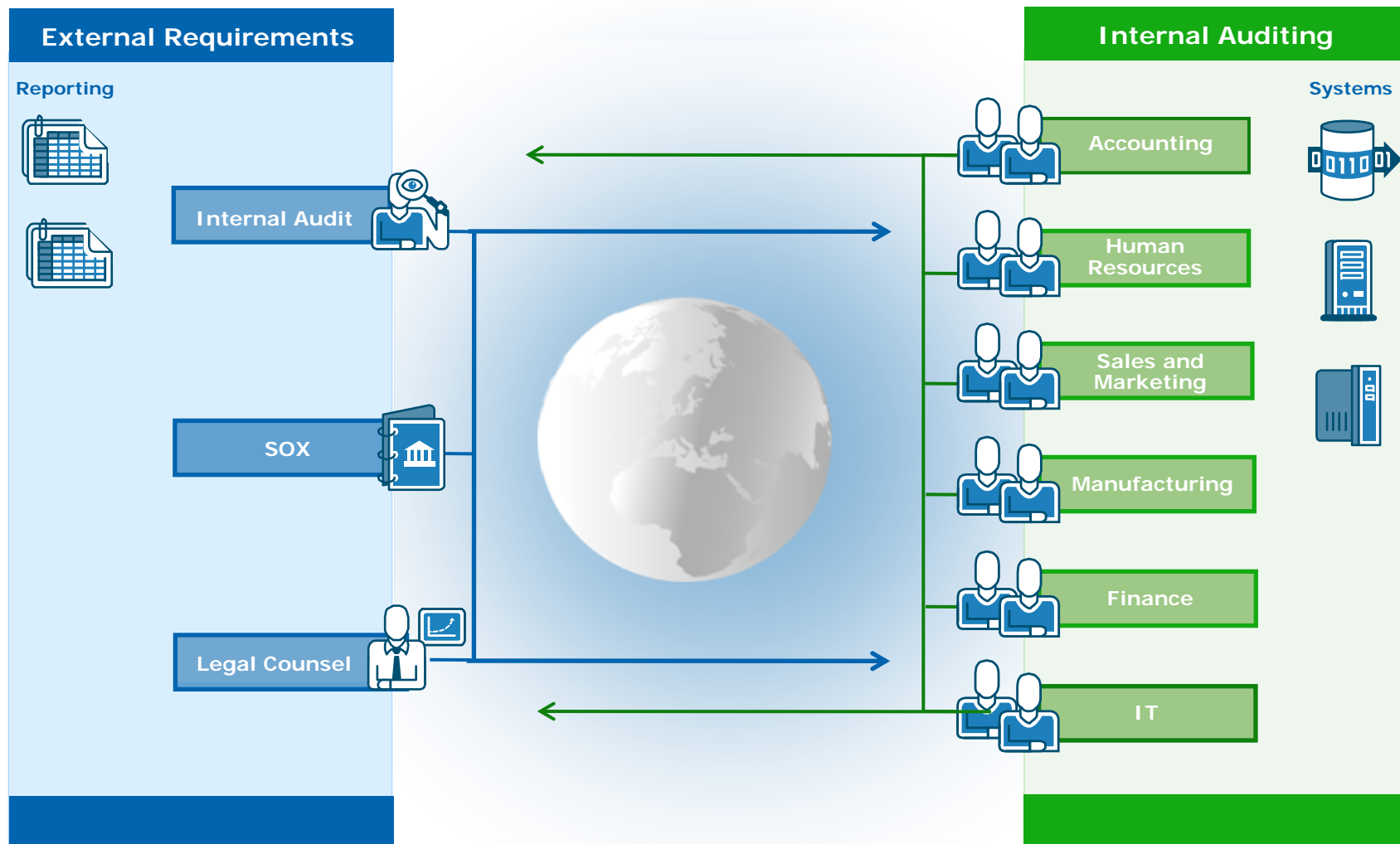


Enter SOX



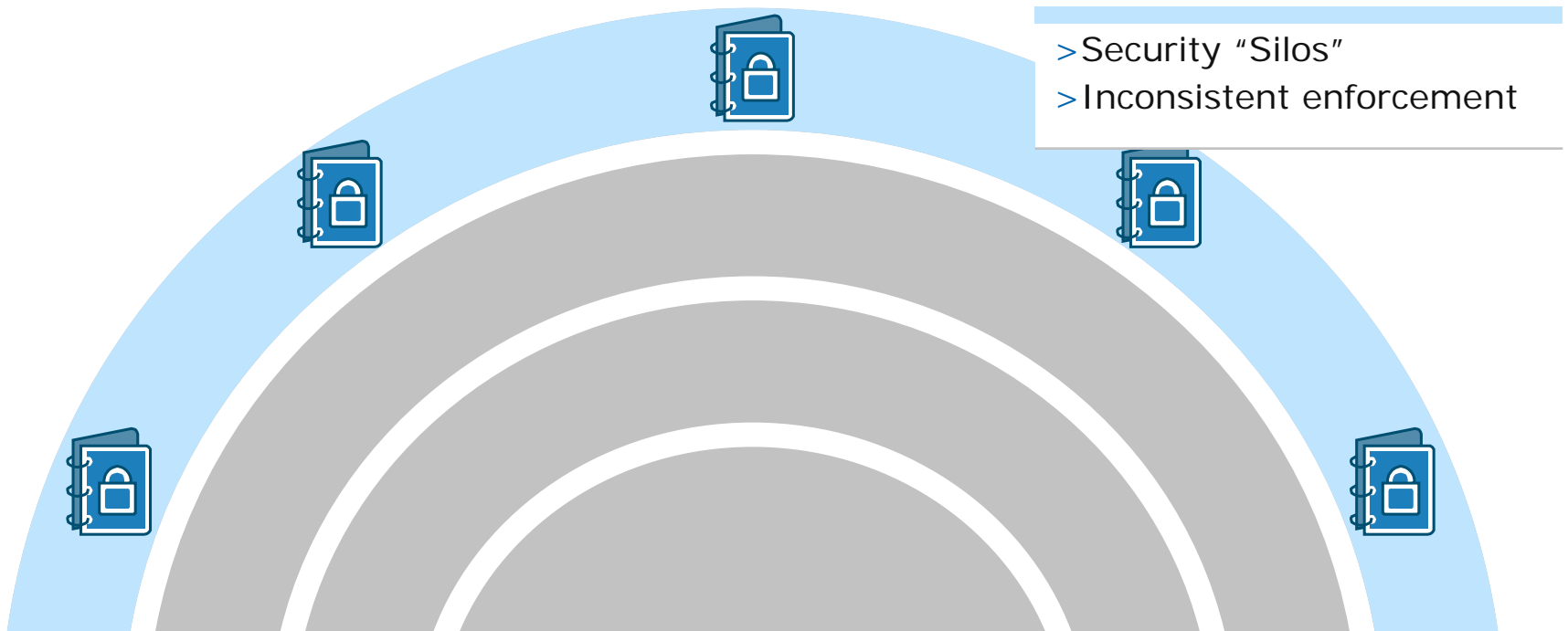


Next Come PCI, EU Privacy Directive, Internal Policies (as well as Compliance Management)





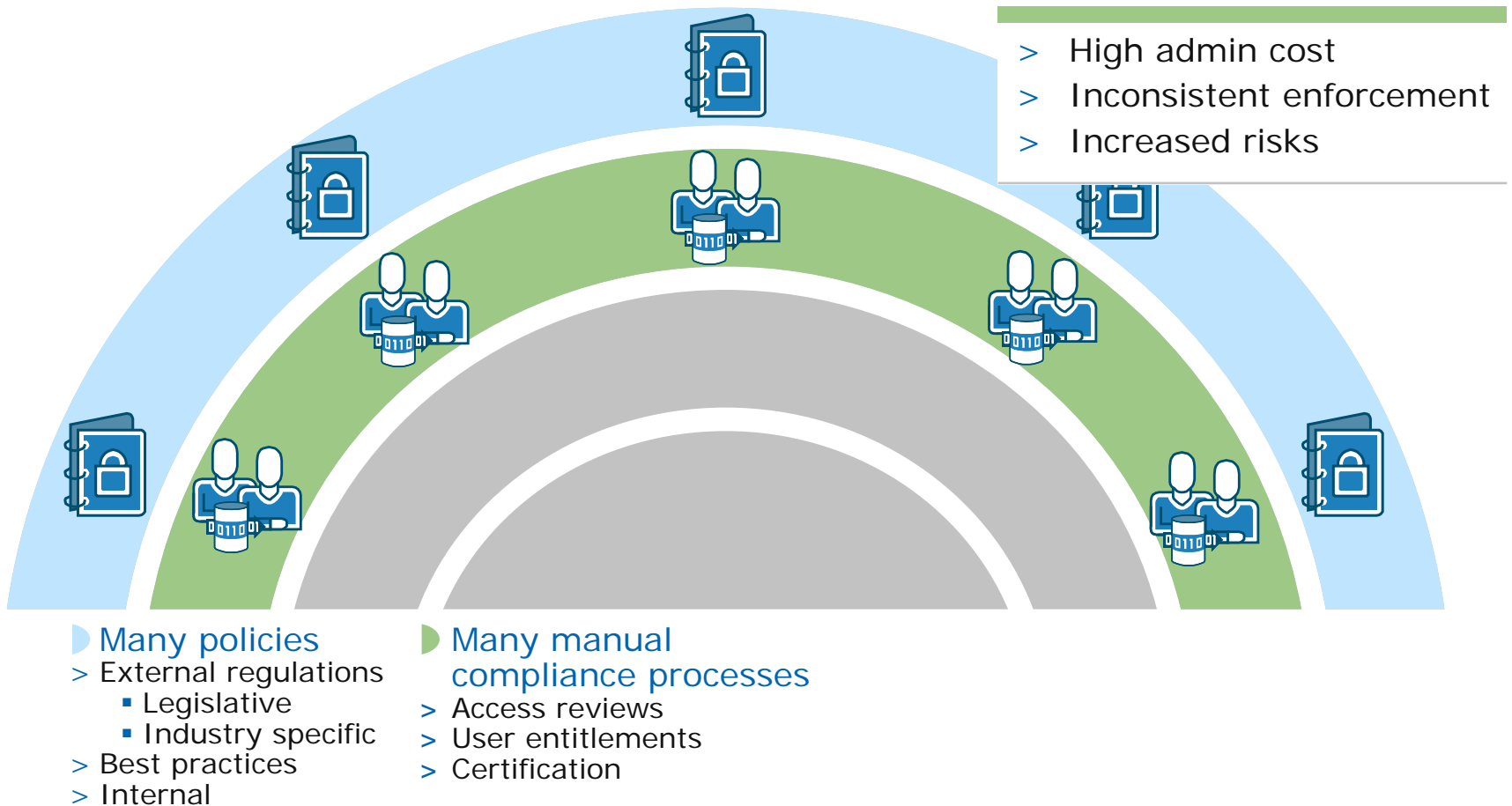
The Challenge of Managing Multiple Users and their Entitlements



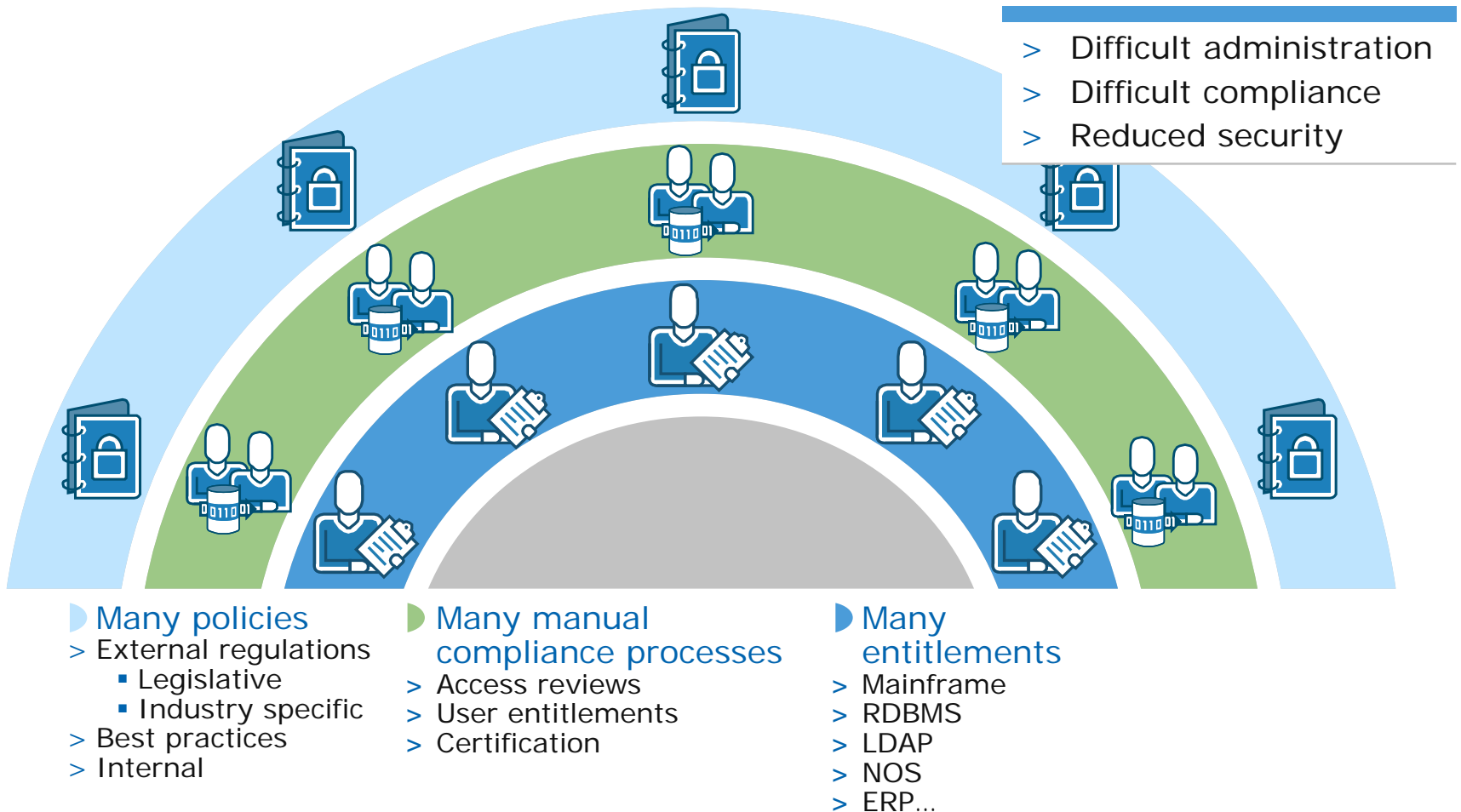
- ▶ Many policies
 - > External regulations
 - Legislative
 - Industry specific
 - > Best practices
 - > Internal



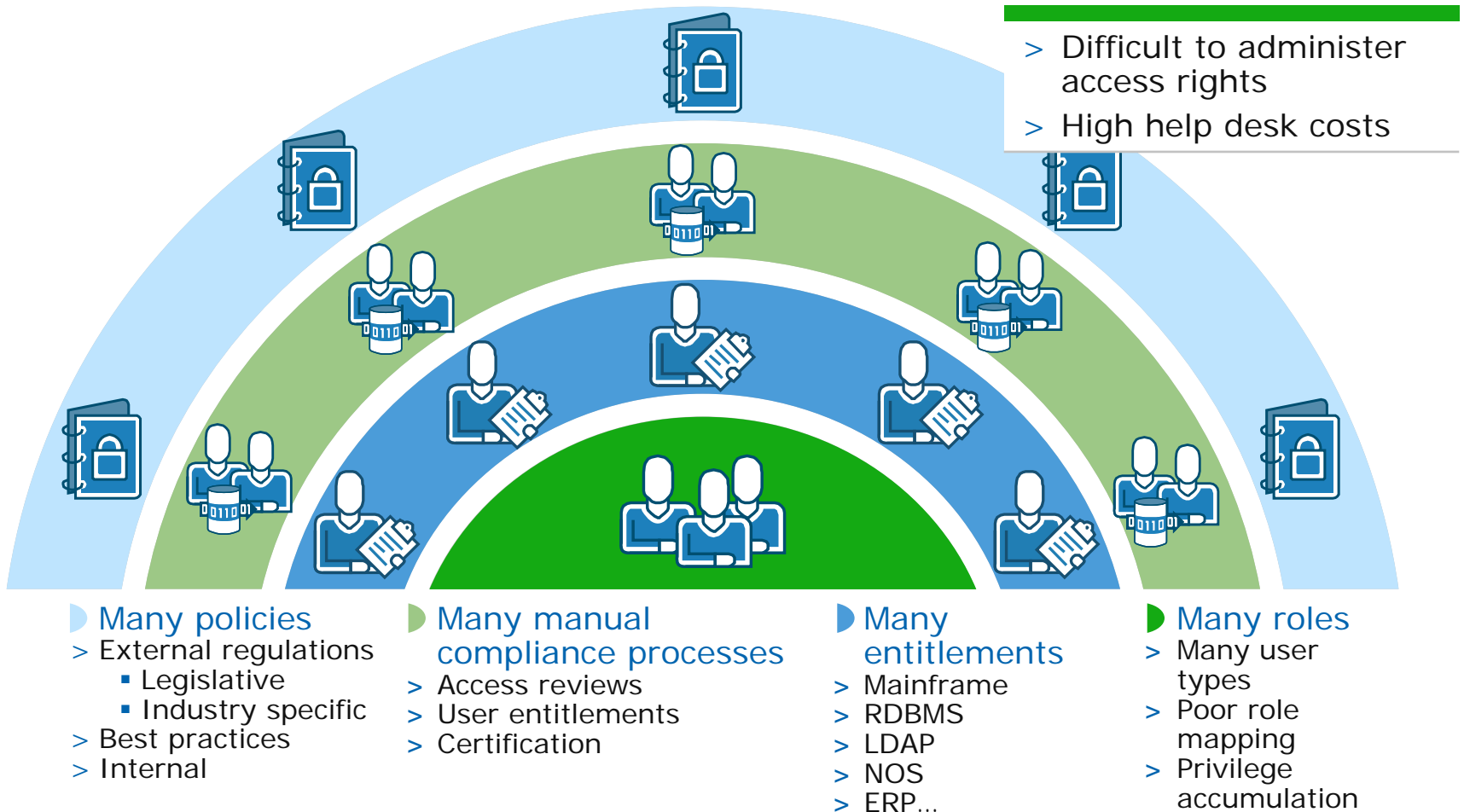
The Challenge of Managing Multiple Users and their Entitlements



The Challenge of Managing Multiple Users and their Entitlements



The Challenge of Managing Multiple Users and their Entitlements





Identity Lifecycle Management

The Solution



► Centralized policies

- > External regulations
- > Legislative
- > Consistent security & industry specific
- > Best practices
- > Internal

► Security compliance automation processes

- >> Reduced admin costs
- >> Risk reduction
- > Certification

► Reduced entitlements

- > Mainframe
- > AD/MS
- > Reduced costs
- > NoS
- > Easier for easier compliance

► Reduced roles

- > Many user efficacy
- > Appropriate enabling
- > Privilege accumulation

Identity Lifecycle Management



Identity Lifecycle Management Defined

Goal: Automating identity-related processes that span the entire enterprise

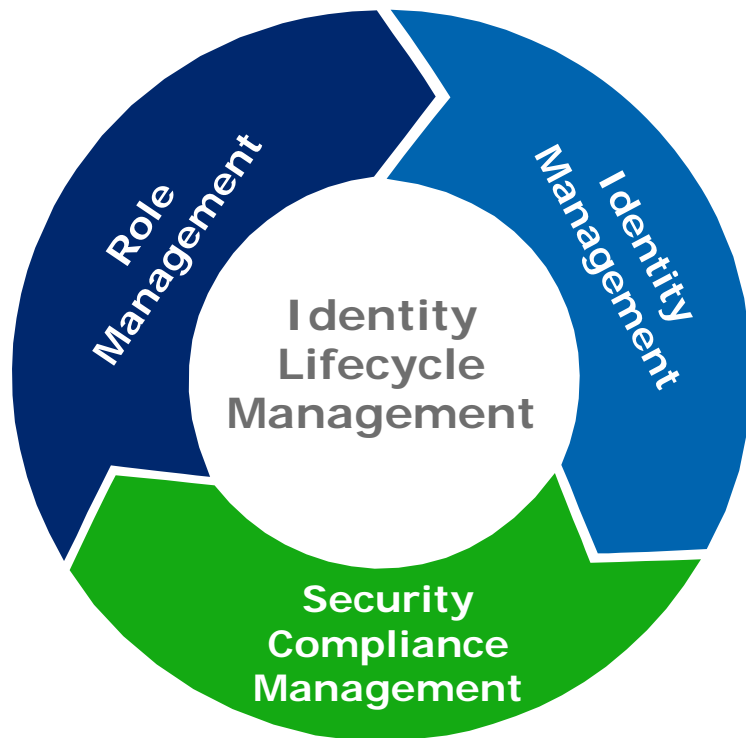
> What are “identity-related” processes?

- On-boarding/Off-boarding an employee
- Users managing their own profiles
- Executing proper provisioning approval processes
- Ensuring user entitlements match functional responsibilities
- Validating company is in compliance
- And more...



Identity Lifecycle Management

IT Needs



Role Management

- Understand what roles exist in the enterprise
- Establish role model that fits organization
- Analyze and maintain role model as business evolves

Identity Management

- Assign users to roles
- Apply role-based controls
- Provision users with approved accounts and privileges
- Manage change requests and approvals over time

Security Compliance Management

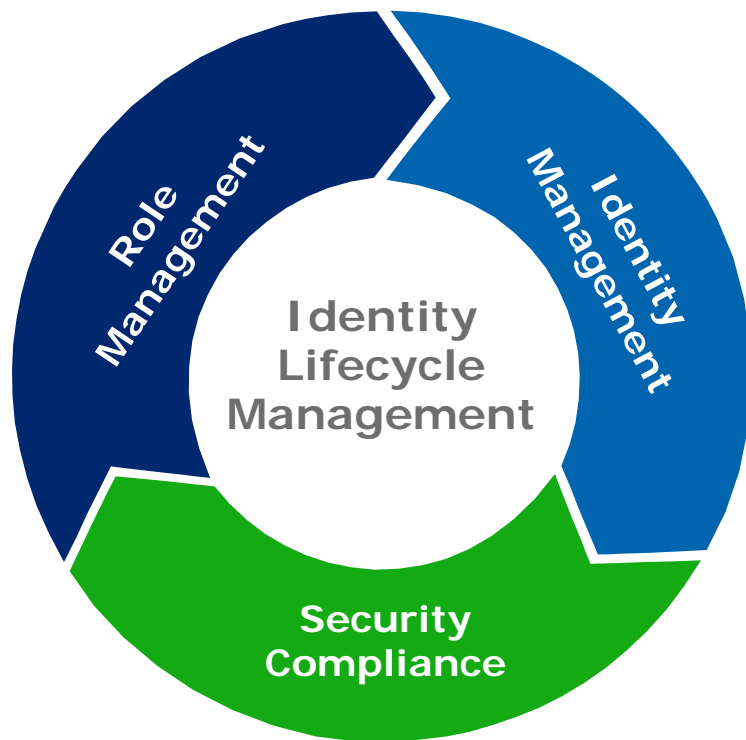
- Understand security policy
- Import audit/log data
- Import identity information
- Compare, then initiate and verify remediation
- Streamline security compliance processes



Identity Lifecycle Management

CA Approach

A complete approach: Enable users faster, reduce costs and risks, support compliance goals



Role Management

- Role discovery
- Maintain role model
- Role analysis and reporting

Identity Management

- Provisioning / De-provisioning
- User self-service
- Identity administration

Security Compliance

- Compliance reporting and dashboards
- User and role entitlement certification
- Initiate change management and validation



Role Mining/Management

Enables efficient and accurate identity and entitlement management

> Role Mining

- Automates discovery of roles and access patterns
- Enables gap analysis, cleanup and role modeling

> Ongoing Role Management

- Processes role approval/adaptation, self service requests
- Detects business changes that affect role structure

> Auditing and Reporting

- Assesses role exceptions, cleanup and repair
- Provides executive reporting and audit trail







Role Management Key Capabilities

The Secret Ingredient – Pattern Recognition Analysis

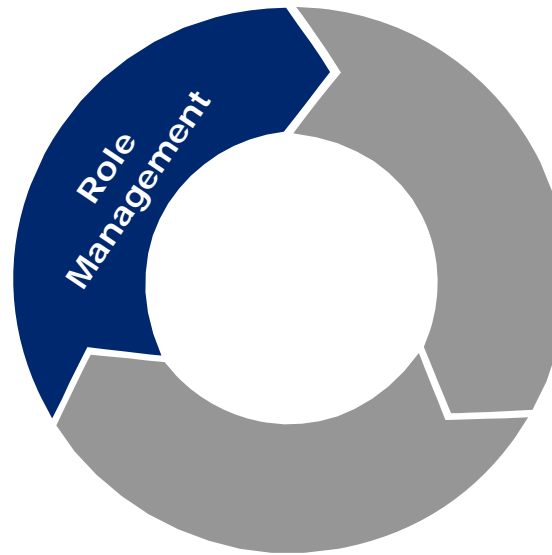

➤ **Audit/Gap Analysis**
Assess and audit systems for exceptions




➤ **Role Modeling**
Reveal methodology
Define roles –
top down
bottom-up



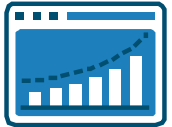
➤ **Policy Modeling**
Verify, certify,
and report
Enriches
provisioning processes



➤ **Data Cleanup Validation and Remediation**
Clean and match user IDs
Identify out of pattern and exceptional users



➤ **Model Management and Reporting Integration**
Detect changes and exceptions
Adapt role based model





Identity Management

Central engine for identity-related processes

> Provisioning/De-Provisioning

- Quickly assigns and removes access privileges
- Automates consistent workflow processes

> User Self Service

- Empowers end users to resolve issues
- Reduces burden on IT and help desk

> Identity Administration

- Centralizes data/policy for consistency across enterprise
- Delegates decision-making to application owners





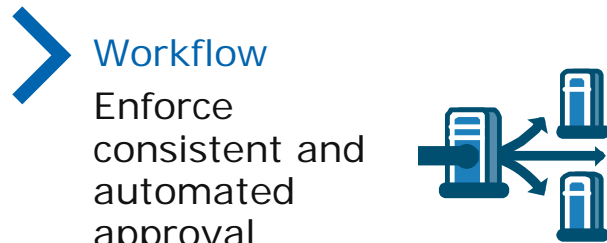
Identity Management Key Capabilities

The Secret Ingredient: Modular yet Integrated



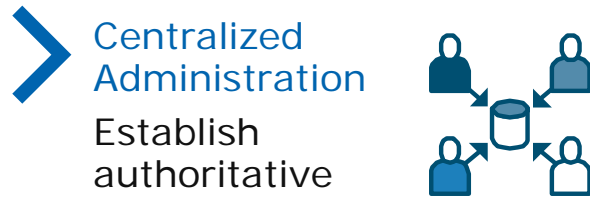
> Role-based Provisioning/De-Provisioning

Ensure timely access and protect sensitive resources



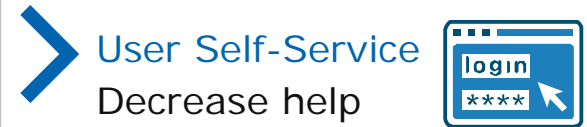
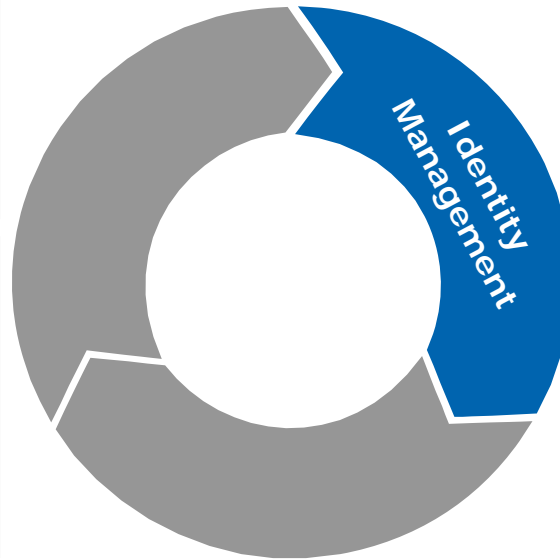
> Workflow

Enforce consistent and automated approval processes



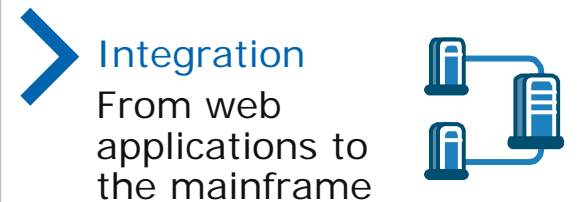
> Centralized Administration

Establish authoritative identity source



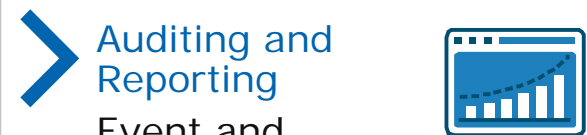
> User Self-Service

Decrease help desk costs and improve user satisfaction



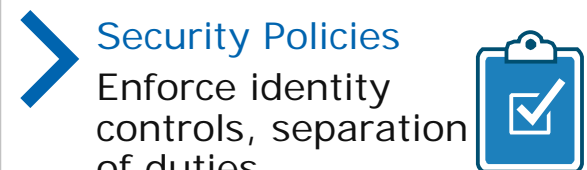
> Integration

From web applications to the mainframe



> Auditing and Reporting

Event and entitlements tracking



> Security Policies

Enforce identity controls, separation of duties



Security Compliance

Meet compliance objectives on a continuous basis

> Compliance Reporting and Dashboards

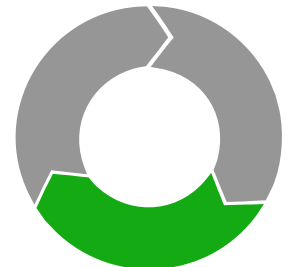
- Generates access, entitlement and audit reports
- Cross-system compliance reporting

> User and Role Entitlement Certification

- Validates users' access is appropriate for their role
- Ensures access to applications is appropriate

> Change Management and Validation

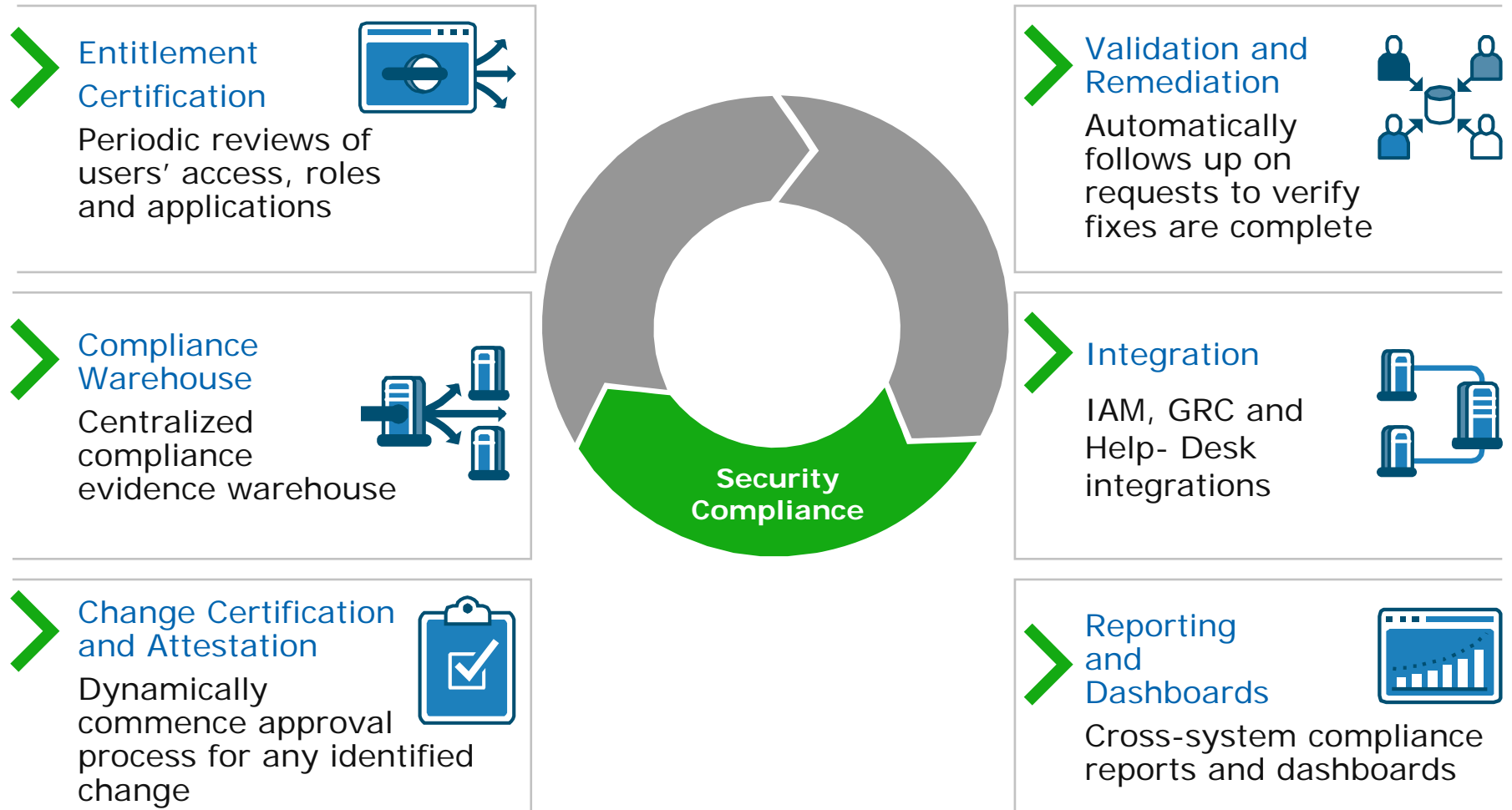
- Initiates change management requests in other systems
- Enables timely follow-up on remediation requests





Security Compliance Key Capabilities

The Secret Ingredient: Process-centric Platform





Identity Lifecycle Management Payoff

- > Increased security and reduced risk
 - Eliminate unauthorized access and orphan accounts
 - Easier to prove compliance
- > Reduced cost/increased productivity
 - Automation, delegation and self-service
 - Overcome idle users requesting help desk support
 - Consolidation of roles accelerates provisioning
- > Improved user experience/satisfaction
 - Faster & easier access to applications and data
- > Centralized hub for storing all security compliance info
 - Provides ongoing visibility and project management over access review processes



CA Customer Successes

Identity Lifecycle Management

> Problems

- Organizations with more roles than users
- 10+ days to provision new employees
- Very complex IT environments:
 - 100+ target systems, 150K roles, 200K identities
- Man weeks to complete compliance processes such as access reviews (multiple man-weeks)

> CA Solutions

- Reduce 150K roles to <5K roles
- Provision new employees in <1 day to multiple systems
- Complete access reviews in hours not days





Summary

- > CA can streamline and automate your existing identity lifecycle management processes for:
 - Identity management
 - Role mining and management
 - Security compliance
- > CA has a complete, integrated solution to manage the entire identity lifecycle across your enterprise

Q&A

